The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID GUNTER and LEEON MOSHE SHACHAF

Appeal No. 2005-2474
Application 09/274,294

ON BRIEF

Before THOMAS, JERRY SMITH, and DIXON, Administrative Patent Judges.

THOMAS, Administrative Patent Judge.

DECISION ON APPEAL

Appellants has appealed to the Board from the examiner's final rejection of claims 1 through 20. Since the examiner has allowed claims 7 through 15 and 19 at pages 8 and 9 of the answer, claims 1 through 6, 16 through 18 and 20 remain for our decision on appeal.

Representative claim 1 is reproduced below:

1. A method for inspecting an encrypted data stream being transferred over a network between two endpoints the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

The following references are relied on by the examiner:

Shwed et al. 5,835,726 Nov. 10, 1998

Schneier Bruce, Applied Cryptography, 1996, John Wiley & Sons, Inc. Second Edition, pg. 13-48.

Claims 1 and 4 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Shwed. Claims 2, 3, 5, 6, 16 through 18 and 20 stand rejected under 35 U.S.C. § 103 as being obvious over the combination of Shwed in view of Schneier.

Rather than repeat the positions of the appellants and examiner, reference is made to the brief and reply brief for appellants' positions, and to the answer for the examiner's positions.

OPINION

We reverse the separate rejections of the noted claims under 35 U.S.C. § 102 and 35 U.S.C. § 103.

As noted at the top of page 4 of the specification as filed, conventional virtual private network (VPN) protocols permit private encryption between two endpoints over a public network and prevent all intermediate data stream inspection of plaintext information even for legitiment purposes, such as for viruses, and scanning or implementation of policy-based access controls. The ability to perform this inspection is provided by the claimed intermediaries, such as the disclosed firewalls and proxy servers in specification Figure 2.

It is this inspection ability that is provided in the broadest claim on appeal, independent claim 1, which first provides a secure transferring of a session key pertinent to each of the endpoints to a intermediary having access to this encrypted data stream using a session key known to both endpoints. Significantly, this claim requires "decrypting the encrypted data stream at the intermediary using the session key" followed by the step of formally inspecting the data stream

after this decryption. Corresponding features are recited in independent claim 20. The remaining independent claims on appeal, claims 5 and 16, do not formally recite per se inspecting the data stream by an intermediary but do so in other words. These claims require that the intermediary decrypt an encrypted session key between the endpoints as recited in representative claim 1 on appeal at, for example, the end of independent claim 5 on appeal and the last clause of independent claim 16 on appeal.

Because of the ability to decrypt and therefore either indirectly or directly inspect the plaintext data stream, it appears that this intermediary is a trusted intermediary. Because the disclosed invention such as in representative Figure 2 and the flow diagram in the disclosed Figure 4 directly teaches that there is a trusted or an encrypted/decrypted data path between each endpoint and the intermediary, this feature is either directly or indirectly recited in each independent claim on appeal. It is at this point that the examiner's positions with respect to Shwed and the combination of Shwed and Schneier fail to teach or suggest the invention in independent claims 1, 5, 16 and 20 on appeal.

At page 10 of the answer the examiner takes the position that the broadest reasonable interpretation of the claimed endpoints corresponds to the respective firewalls in Figure 16 of Shwed acting as both intermediaries and endpoints, which is a position more refined than the boarder approach taken in the statement of the rejection as to independent claim 1 at page 4 of the answer where the examiner asserts that the endpoints in Shwed are secured by two firewalls, which the examiner considers to be the claimed intermediaries. On the other hand, claim 1 requires two endpoints AND an intermediary. Therefore, the two firewalls in Figure 16 of Shwed can't be both endpoints and the intermediaries.

This analysis of ours is consistent with what appellants urge at pages 3 through 6 of the reply brief which we reproduce here:

> (2) The Cited Reference of Shwed Does Not Disclose an Encrypted Data Stream Transferred Between Endpoints and an Intermediary Having Access to Both Endpoints.
>
> The Examiner relies on the reference U.S. Patent 5,835,726 to Shwed et al (hereinafter, "Shwed") as disclosing firewalls that may "act[ing] as both intermediaries and endpoints". The examiner argues that his
>
> > broadest reasonable interpretation of claimed endpoints corresponds to Firewall 1 and Firewall 2 of Shwed acting as both intermediaries and endpoints. That is Firewall 1 and Firewall 2 both

> act as secure pathway for host1 and host2 as well a an intermediary to examine the data packet flowing from host 1 to host 2 or vice versa. In other words, the Firewall 1 is a source of transmitting encrypted packet(i.e. and endpoint) to intermediary firewall 2, while it is also an intermediary point for inspecting packets received from host 2. The Examiner responds that Firewall 1 with respect to firewall 2 is an endpoint relative to firewall acting as an intermediary.

Appellant disagrees. The present invention describes and claims distinctive endpoints and an intermediary. The Examiner inappropriately combines one of the firewalls described in Shwed as one of the endpoints and as an intermediary. In the Examiner's interpretation, the firewalls of Shwed are both the endpoints and the intermediaries. The client computers (i.e., host1 and host 2) in Shwed are not endpoints since they do not perform or pass encrypted communication; however, in the Examiner's interpretation at least one of the client computers must be an endpoint if one of the firewalls acts as an intermediary. In other words, if host 2 is sending packets to firewall 1 which receives and inspects the packets, where firewall 1 acts as an intermediary and endpoint to host 2, then host 2 must be considered an endpoint. Shwed discloses that the client computers never encrypt the data or directly communicate with one another which the present invention particularly discloses and claims. Shwed relies on firewalls 1 and 2 to perform the communicating and encrypting. The Examiner's interpretation of Shwed provided that only the firewalls are considered as endpoints, which leads to two entities (i.e., firewall 1 and 2) encrypting data and communicating with one another, without the provision of a third entity (i.e., intermediary) to inspect the encrypted data as disclosed and recited in the claims of the present invention.

(3) The Cited Reference of Shwed Does Not Disclose the Host Computers As Endpoints.

> As discussed above, in view of the Examiner's interpretation of Shwed, the host computers (i.e., host 1 and host 2) cannot be considered endpoints, since the host computers of Shwed do not negotiate, generate, and exchange a session key. Furthermore, the host computers do not communicate an "encrypted data stream". The firewalls of Shwed perform these functions, not the host computers.
>
> In the Examiner's arguments and scenarios that recite Shwed, a first host computer is considered an endpoint to a first firewall that is considered as a second endpoint to the first host computer. As disclosed in Shwed, unencrypted and unprotected data from the first host computer is sent to a second firewall which encrypts the data and sends it to the first firewall. Since the host computers in Shwed do not encrypt the data or negotiate, generate, and exchange a session key, the host computers can not be considered as endpoints.
>
> As discussed above, the Examiner interprets that the firewalls of Shwed are considered as endpoints and intermediaries. This is particularly illustrated in the Examiner's rejections of claims 2, 3, 5-6 and 16-18 that "Shwed does not suggest or teach a session key known to both endpoints ... The Examiner responds that Shwed's session key R is known to Firewall 1 and Firewall 2".
>
> Therefore, in this interpretation of the Examiner, Firewall 1 and Firewall 2 are the endpoints which precludes that neither of the host computers may be endpoints.

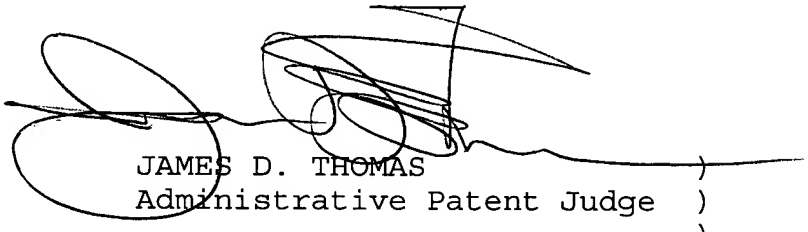
Shwed does not contemplate the kind of trusted intermediary as we outlined earlier. The background discussion of Figure 16 begins at the bottom of column 12 in this reference. The following discussion associated with Figure 16 and the additional embodiment shown in Figure 21 and discussed in the latter columns of this reference fails to teach or suggest the trusted

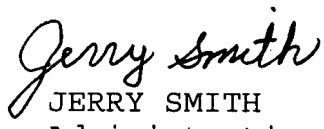
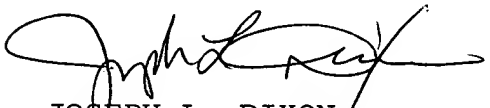
intermediary to the extent recited in each of the independent claims on appeal as explained earlier. Figure 21 is a variation of the showing in Figure 16. Each of the respective claimed endpoints requires an ability to encrypt and decrypt information in addition to a corresponding ability in a recited intermediary, the features of which are not shown in either Figure 16 or Figure 21 since each of the respective hosts or PCs in these figures do not contain the ability to encrypt and decrypt information with respect to their corresponding firewalls, which perform the encryption and decryption capabilities for respective hosts.

As to the separate rejection of independent claims 5, 16 and 20 under 35 U.S.C. § 103 in view of Shwed and Schneier, even if these references are properly combinable to enhance the session key teachings of Shwed by those of Schneier as argued by the examiner, the noted deficiencies of Shwed do not yield the claimed invention set forth in each of these independent claims on appeal as well as dependent claims 2 and 3 of independent claim 1. In other words, the deficiencies of Shwed are not made up for or compensated for by the teachings and showings of Schneier.

In view of the foregoing, the decision of the examiner rejecting various claims on appeal under 35 U.S.C. § 102 and 35 U.S.C. § 103 is reversed.

REVERSED



JAMES D. THOMAS)
Administrative Patent Judge)
)

)
JERRY SMITH) BOARD OF PATENT
Administrative Patent Judge) APPEALS AND
) INTERFERENCES

)
JOSEPH L. DIXON)
Administrative Patent Judge)

JDT:pgc

Appeal No. 2005-2474
Application 09/274,294

Lee & Hayes PLLC
421 W. Riverside Avenue
Suite 500
Spokane, WA 99201